

ON CUBIC EQUATIONS OVER p -ADIC FIELD

FARRUKH MUKHAMEDOV, BAKHROM OMIROV, AND MANSOOR SABUROV

ABSTRACT. We provide a solvability criteria for a depressed cubic equation in domains $\mathbb{Z}_p^*, \mathbb{Z}_p, \mathbb{Q}_p$. We show that, in principal, the Cardano method is not always applicable for such equations. Moreover, the numbers of solutions of the depressed cubic equation in domains $\mathbb{Z}_p^*, \mathbb{Z}_p, \mathbb{Q}_p$ are provided. Since $\mathbb{F}_p \subset \mathbb{Q}_p$, we generalize J.-P. Serre's [27] and Z.H.Sun's [28, 30] results concerning with depressed cubic equations over the finite field \mathbb{F}_p . Finally, all depressed cubic equations, for which the Cardano method could be applied, are described and the p -adic Cardano formula is provided for those cubic equations.

Mathematics Subject Classification: 11Sxx

Key words: Depressed cubic equation, p -adic number, Solvability criterion, p -adic Cardano formula;

1. INTRODUCTION

In principal, according to Ostrowski's theorem (see [10],[15],[25]), there are only two types of absolute values on the field of rational numbers \mathbb{Q} : Archimedean or the real absolute value $|\cdot|_\infty$ and non-Archimedean or the p -adic absolute value $|\cdot|_p$ for some prime number p . These topological differences influence algebraic structures of the real and p -adic number fields $\mathbb{R} \equiv \overline{\mathbb{Q}}^{|\cdot|_\infty}$, $\mathbb{Q}_p \equiv \overline{\mathbb{Q}}^{|\cdot|_p}$.

Over the last century, p -adic numbers and p -adic analysis have come to play a central role in modern number theory. This importance comes from the fact that they afford a natural and powerful language for talking about congruences between integers, and allow the use of methods borrowed from analysis for studying such problems.

The fields of p -adic numbers were introduced by German mathematician K. Hensel [11]. The p -adic numbers were motivated primarily by an attempt to bring the ideas and techniques of the power series into number theory. Their canonical representation is analogous to the expansion of analytic functions into power series. This is one of the manifestations of the analogy between algebraic numbers and algebraic functions.

For a fixed prime p , by \mathbb{Q}_p it is denoted the field of p -adic numbers, which is a completion of the rational numbers \mathbb{Q} with respect to the non-Archimedean norm $|\cdot|_p : \mathbb{Q} \rightarrow \mathbb{R}$ given by

$$|x|_p = \begin{cases} p^{-r} & x \neq 0, \\ 0, & x = 0, \end{cases} \quad (1.1)$$

here, $x = p^r \frac{m}{n}$ with $r, m \in \mathbb{Z}$, $n \in \mathbb{N}$, $(m, p) = (n, p) = 1$. A number r is called a p -order of x and it is denoted by $ord_p(x) = r$.

Any p -adic number $x \in \mathbb{Q}_p$ can be uniquely represented in the following canonical form

$$x = p^{\text{ord}_p(x)} (x_0 + x_1 \cdot p + x_2 \cdot p^2 + \cdots)$$

where $x_0 \in \{1, 2, \dots, p-1\}$ and $x_i \in \{0, 1, 2, \dots, p-1\}$, $i \geq 1$, (see [6], [15])

More recently, numerous applications of p -adic numbers have shown up in theoretical physics and quantum mechanics (see for example, [1], [5], [9], [12, 13], [17]-[21], [31, 32]).

The p -adic numbers are connected with solutions of Diophantine equations modulo increasing powers of a prime number. The study of Diophantine equations is finding solutions of polynomial equations or systems of equations in integers, rational numbers, or sometimes more general number rings. Such a topic is one of the oldest branches of number theory, in fact of mathematics itself. The theory of Diophantine equations in number rings was well developed in [6], [8].

One of the simplest Diophantine equation is the following equation

$$x^q = a \tag{1.2}$$

over \mathbb{Q}_p , where $q \in \mathbb{N}$, $a \in \mathbb{Q}_p$. The solvability criterion for the equation (1.2) from algebraic number theory point of view was provided in [16], [23], [26]. However, surprisingly, this criterion was not mentioned in the Bible books of the p -adic analysis (see [10], [15], [25]) except $q = 2$. From p -adic analysis point of view, the solvability criterion for the equation (1.2) for any $q \in \mathbb{N}$ was provided in [3, 4], [7], [22].

All of us are aware that there is a criterion for the solvability of any quadratic equation $ax^2 + bx + c = 0$ in \mathbb{Q}_p , where $a, b, c \in \mathbb{Q}_p$ with $a \neq 0$. It can be derived by the method of completing the square as follows. Without loss any generality, we may consider the following quadratic equation $x^2 + qx + r = 0$, where $q = \frac{b}{a}$, $r = \frac{c}{a}$. We then have that $(x + \frac{q}{2})^2 = (\frac{q}{2})^2 - r$. This equation has a solution in \mathbb{Q}_p if and only if $\log_p \left| \left(\frac{q}{2} \right)^2 - r \right|_p$ is an even number and $\left(\left| \left(\frac{q}{2} \right)^2 - r \right|_p \left(\left(\frac{q}{2} \right)^2 - r \right) \right)^{\frac{p-1}{2}} \equiv 1 \pmod{p}$ for $p > 2$ or $\left| \left(\frac{q}{2} \right)^2 - r \right|_2 \left(\left(\frac{q}{2} \right)^2 - r \right) \equiv 1 \pmod{8}$ for $p = 2$. Thus, the solutions of the quadratic equation can be given in the form of $x_{\pm} = -\frac{q}{2} \pm \sqrt{\left(\frac{q}{2} \right)^2 - r}$.

Unlike real numbers \mathbb{R} , in general, the cubic equation $ax^3 + bx^2 + cx + d = 0$ is not necessary to have a solution in \mathbb{Q}_p , where $a, b, c, d \in \mathbb{Q}_p$ with $a \neq 0$. For example, the following simple cubic equation $x^3 = p$ does not have any solution in \mathbb{Q}_p . Therefore, it is a natural to find some criterion for solvability of the cubic equation in \mathbb{Q}_p . One of the general way to find solutions of the cubic equation in a local field is the Cardano method. However, by means of the Cardano method, we could not tell an existence of solutions of all cubic equations. Let us illustrate it in the following example.

We consider the following cubic equation $x^3 - \frac{3}{p}x + \frac{p-3}{p} = 0$ in \mathbb{Q}_p , where $p > 3$. It is clear that this cubic equation has a solution $x_* = -1$. However, the Cardano method is not applicable for this equation. In fact, let us search for a solution in the form of $x = u + v$. After elementary calculations, we obtain the following system of

equations

$$\begin{cases} uv = \frac{1}{p} \\ u^3 + v^3 = -\frac{p-3}{p} \end{cases}$$

In order to solve this system, we should solve the following quadratic equation $z^2 + \frac{p-3}{p}z + \frac{1}{p^3} = 0$ in \mathbb{Q}_p , where $z = u^3$. However, $\log_p \left| \left(\frac{p-3}{2p} \right)^2 - \frac{1}{p^3} \right|_p = 3$ is odd. Thus, this quadratic equation $z^2 + \frac{p-3}{p}z + \frac{1}{p^3} = 0$ does not have solutions in \mathbb{Q}_p . Therefore, in general, by means of Cardano method we could not detect solutions of all cubic equations.

To the best of our knowledge, we could not find the solvability criterion in an explicit form for the cubic equation (1.3) in the Bible books of p -adic analysis and algebraic number theory (see [2], [10], [15], [16], [23], [25], [26]). Some sufficient conditions for the solvability of the cubic equation (1.3) in \mathbb{Q}_p were provided in [3, 4], [23].

In this paper, we provide the criterion for solvability of any cubic equation $ax^3 + bx^2 + cx + d = 0$ in \mathbb{Q}_p where $a, b, c, d \in \mathbb{Q}_p$ with $a \neq 0$. Dividing by a and substituting x by $x - \frac{b}{3a}$ we can get the so-called *depressed cubic* equation

$$x^3 + ax = b \tag{1.3}$$

Concerning with classification problems of finite dimensional Leibniz algebras (see [14]), in this paper, we are going to provide the criterion for the solvability of the depressed cubic equation (1.3), where $a, b \in \mathbb{Q}_p$, in domains \mathbb{Z}_p^* , \mathbb{Z}_p , \mathbb{Q}_p . In general case, one can easily derive the criterion from the depressed cubic equation.

It is worth mentioning that there are some cubic equations which do not have any solutions in \mathbb{Z}_p^* (in \mathbb{Z}_p) but have solutions in \mathbb{Z}_p (in \mathbb{Q}_p).

Let us consider the following equation $x^3 + p^2x = 2p^3$ in \mathbb{Q}_p . This equation does not have any solutions in \mathbb{Z}_p^* . In fact, for any $x \in \mathbb{Z}_p^*$ one has that $|x^3 + p^2x|_p = 1$. On the other hand, $|2p^3|_p < 1$. This contradictions shows that the cubic equation $x^3 + p^2x = 2p^3$ does not have any solution in \mathbb{Z}_p^* . However, it has a solution $x_* = p$ which belongs to \mathbb{Z}_p .

Let us consider the following equation $x^3 + p^2x = \frac{1+p^4}{p^3}$ in \mathbb{Q}_p . If $x \in \mathbb{Z}_p$ then $|x^3 + p^2x|_p \leq 1$. However, $\left| \frac{1+p^4}{p^3} \right|_p > 1$. This means that the equation $x^3 + p^2x = \frac{1+p^4}{p^3}$ does not have any solution in \mathbb{Z}_p . On the other hand, this equation has a solution $x_* = \frac{1}{p}$ which belongs to \mathbb{Q}_p .

Therefore, finding the criterion for the solvability of the depressed cubic equation (1.3), where $a, b \in \mathbb{Q}_p$, in domains \mathbb{Z}_p^* , \mathbb{Z}_p , \mathbb{Q}_p is of independent interest.

Let us consider the depressed cubic equation (1.3) in the finite field $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$

$$x^3 + ax = b, \tag{1.4}$$

where $a, b, x \in \mathbb{F}_p$. By $\mathbf{N}_{\mathbb{F}_p}(x^3 + ax - b)$, we denote the number of solutions of the depressed cubic equation (1.4) in \mathbb{F}_p , where $a, b \in \mathbb{F}_p$.

If $a = \bar{0}$ or $b = \bar{0}$ then $\mathbf{N}_{\mathbb{F}_p}(x^3 + ax - b)$ can be easily study. Therefore, we shall assume that $a \neq \bar{0}$ and $b \neq \bar{0}$.

The study of $\mathbf{N}_{\mathbb{F}_p}(x^3 + ax - b)$ goes back to several centuries with contributions from Euler, Gauss, Jacobi, Cauchy. Surprisingly, up to now, there are still many papers which were devoted to study $\mathbf{N}_{\mathbb{F}_p}(x^3 + ax - b)$ (see papers [27], [28, 30], and references therein)

We denote the number of solutions of the depressed cubic equation (1.3), where $a, b \in \mathbb{Q}_p$, in domains \mathbb{Z}_p^* , \mathbb{Z}_p , \mathbb{Q}_p respectively by $\mathbf{N}_{\mathbb{Z}_p^*}(x^3 + ax - b)$, $\mathbf{N}_{\mathbb{Z}_p}(x^3 + ax - b)$, $\mathbf{N}_{\mathbb{Q}_p}(x^3 + ax - b)$. In this paper we shall give the description of all these sets whenever $a, b \in \mathbb{Q}_p$. Since $\mathbb{F}_p \subset \mathbb{Q}_p$, our results generalize all results in [27], [28, 30] which were concerning with equation (1.4) in \mathbb{F}_p .

The last but not least, as we already mentioned that the Cardano method is not applicable for all depressed cubic equations (1.3), where $a, b \in \mathbb{Q}_p$. Therefore, in the last section we are going to describe all depressed cubic equations for which the Cardano method can be applied and we shall provide p -adic Cardano formula for those equations.

2. PRELIMINARIES

In this section we shall recall some necessary results from number theory.

We respectively denote the set of all p -adic integers and units of \mathbb{Q}_p by

$$\mathbb{Z}_p = \{x \in \mathbb{Q}_p : |x|_p \leq 1\}, \quad \mathbb{Z}_p^* = \{x \in \mathbb{Q}_p : |x|_p = 1\}.$$

Any p -adic unit $x \in \mathbb{Z}_p^*$ has the following unique canonical form

$$x = x_0 + x_1 \cdot p + x_2 \cdot p^2 + \dots$$

where $x_0 \in \{1, 2, \dots, p-1\}$ and $x_i \in \{0, 1, 2, \dots, p-1\}$, $i \in \mathbb{N}$.

Any nonzero p -adic number $x \in \mathbb{Q}_p$ has a unique representation of the form

$$x = \frac{x^*}{|x|_p}, \text{ where } x^* \in \mathbb{Z}_p^*.$$

Lemma 2.1 (Hensel's Lemma, [6]). *Let $f(x)$ be polynomial whose the coefficients are p -adic integers. Let θ be a p -adic integer such that for some $i \geq 0$ we have*

$$f(\theta) \equiv 0 \pmod{p^{2i+1}},$$

$$f'(\theta) \equiv 0 \pmod{p^i}, \quad f'(\theta) \not\equiv 0 \pmod{p^{i+1}}.$$

Then $f(x)$ has a unique p -adic integer root x_0 which satisfies $x_0 \equiv \theta \pmod{p^{i+1}}$.

Let p be a prime number, $q \in \mathbb{N}$, $a \in \mathbb{F}_p$ with $a \neq \bar{0}$. The number a is called a q -th power residue modulo p if the the following equation

$$x^q = a \tag{2.1}$$

has a solution in \mathbb{F}_p .

Proposition 2.2 ([24]). *Let p be an odd prime number, $q \in \mathbb{N}$, $d = (q, p-1)$, and $a \in \mathbb{F}_p$ with $a \neq \bar{0}$. Then the following statements hold true:*

- (i) *a is the q -th power residue modulo p if and only if one has $a^{\frac{p-1}{d}} = \bar{1}$;*
- (ii) *If $a^{\frac{p-1}{d}} = \bar{1}$ then the equation (2.1) has d number of solutions in \mathbb{F}_p .*

The solvability criterion of the following equation in \mathbb{Q}_p

$$x^q = a, \quad (2.2)$$

where $q \in \mathbb{N}$, $a \in \mathbb{Q}_p$ with $a \neq 0$, was provided in [3, 4], [7], [16], [22], [23], [26].

Proposition 2.3. *Let p be an odd prime number, $q \in \mathbb{N}$, $a \in \mathbb{Q}_p$, $a = \frac{a^*}{|a|_p}$ and $a^* \in \mathbb{Z}_p^*$ with $a^* = a_0 + a_1 \cdot p + a_2 \cdot p^2 + \dots$. Then the following statements hold true:*

- (i) *If $(q, p) = 1$ then the equation (2.2) has a solution in \mathbb{Q}_p if and only if $a_0^{\frac{p-1}{(q, p-1)}} \equiv 1 \pmod{p}$ and $\log_p |a|_p$ is divisible by q*
- (ii) *If $(q, p) = 1$, $a_0^{\frac{p-1}{(q, p-1)}} \equiv 1 \pmod{p}$ and $\log_p |a|_p$ is divisible by q then the equation (2.2) has $(q, p-1)$ number of solutions in \mathbb{Q}_p .*
- (iii) *If $(q, p) = 1$ then the equation $y^q \equiv a^* \pmod{p^k}$ has a solution in \mathbb{Z}_p^* for some $k \in \mathbb{N}$ if and only if $a_0^{\frac{p-1}{(q, p-1)}} \equiv 1 \pmod{p}$.*
- (iv) *If $q = m \cdot p^s$ with $(m, p) = 1$, $s \geq 1$ then the equation (2.2) has a solution in \mathbb{Q}_p if and only if $a_0^{\frac{p-1}{(m, p-1)}} \equiv 1 \pmod{p}$, $a_0^{p^s} \equiv a \pmod{p^{s+1}}$ and $\log_p |a|_p$ is divisible by q .*

Let us consider the following depressed cubic equation in the field \mathbb{F}_p

$$x^3 + \bar{a}x = \bar{b}, \quad (2.3)$$

where $\bar{a}, \bar{b} \in \mathbb{F}_p$. We assume that $\bar{a} \neq \bar{0}$ and $\bar{b} \neq \bar{0}$. The number of solutions $\mathbf{N}_{\mathbb{F}_p}(x^3 + \bar{a}x - \bar{b})$ of this equation was described in [29].

Proposition 2.4 ([29]). *Let $p > 3$ be a prime number and $\bar{a}, \bar{b} \in \mathbb{F}_p$ with $\bar{a}\bar{b} \neq \bar{0}$. Let $\bar{D} = -4\bar{a}^3 - 27\bar{b}^2$ and $u_{n+3} = \bar{b}u_n - \bar{a}u_{n+1}$ for $n \in \mathbb{N}$ with $u_1 = \bar{0}$, $u_2 = -\bar{a}$, $u_3 = \bar{b}$. Then the following holds true:*

$$\mathbf{N}_{\mathbb{F}_p}(x^3 + \bar{a}x - \bar{b}) = \begin{cases} 3 & \text{if } \bar{D}u_{p-2}^2 = \bar{0} \\ 0 & \text{if } \bar{D}u_{p-2}^2 = 9\bar{a}^2 \\ 1 & \text{if } \bar{D}u_{p-2}^2 \neq \bar{0}, 9\bar{a}^2 \end{cases}$$

It is worth mentioning that $\mathbf{N}_{\mathbb{F}_p}(x^3 + \bar{a}x - \bar{b})$ was studied in [27] for the case $\bar{a} = -\bar{1}$ and $\bar{b} = \bar{1}$.

The proofs of the following statements are straightforward.

Proposition 2.5. *Let $p > 3$ be a prime number and $\bar{a}, \bar{b} \in \mathbb{F}_p$, $\bar{a}\bar{b} \neq \bar{0}$. Let $\bar{D} = -4\bar{a}^3 - 27\bar{b}^2$ and $u_{n+3} = \bar{b}u_n - \bar{a}u_{n+1}$ with $\bar{D}u_{p-2}^2 \neq 9\bar{a}^2$, $u_1 = \bar{0}$, $u_2 = -\bar{a}$, $u_3 = \bar{b}$.*

- I *Let $\bar{D}u_{p-2}^2 = \bar{0}$. Then the following statements hold true:*
 - I.1 *The equation (2.3) has 3 distinct solutions in \mathbb{F}_p if and only if $\bar{D} \neq \bar{0}$. Moreover, one has that $3\bar{x}^2 + \bar{a} \neq 0$ for any root \bar{x} ;*
 - I.2 *The equation (2.3) has 2 distinct solutions in \mathbb{F}_p while one of them of multiplicity 2 if and only if $\bar{D} = \bar{0}$. If \bar{x}_1, \bar{x}_2 are 2 distinct solutions while \bar{x}_1 is a multiple solution then $\bar{x}_1 = \frac{3\bar{b}}{2\bar{a}}$, $\bar{x}_2 = -\frac{3\bar{b}}{\bar{a}}$, and $3\bar{x}_2^2 + \bar{a} \neq \bar{0}$;*
 - I.3 *The equation (2.3) does not have any solution of multiplicity 3.*
- II *Let $\bar{D}u_{p-2}^2 \neq \bar{0}, 9\bar{a}^2$. If \bar{x} is a solution of the equation (2.3) then $3\bar{x}^2 + \bar{a} \neq \bar{0}$.*

Remark 2.1. Due to Proposition 2.5, one may conclude that under the assumption of Proposition 2.5, there always exists at least one solution \bar{x} of the equation (2.3) such that $3\bar{x}^2 + \bar{a} \neq \bar{0}$.

3. THE SOLVABILITY CRITERION IN DOMAINS \mathbb{Z}_p^* , \mathbb{Z}_p , \mathbb{Q}_p WITH $p > 3$

In this section we provide the solvability criterion for the depressed cubic equation (1.3) in domains \mathbb{Z}_p^* , \mathbb{Z}_p , \mathbb{Q}_p with $p > 3$, where $a, b \in \mathbb{Q}_p$ with $ab \neq 0$. The solvability criteria of the equation (1.3) for the case $ab = 0$ is given in [7], [22] (see Proposition 2.3).

We need the following auxiliary result.

Proposition 3.1. *Let p be any prime. Suppose that the equation (1.3) has a solution in \mathbb{Z}_p^* , where $a, b \in \mathbb{Q}_p$ with $ab \neq 0$. Then one of the following conditions holds true:*

- (i) $|a|_p < |b|_p = 1$;
- (ii) $|b|_p < |a|_p = 1$;
- (iii) $|a|_p = |b|_p \geq 1$.

Proof. Let p be any prime. We suppose that the equation (1.3) has a solution in \mathbb{Z}_p^* . Since $ab \neq 0$, one can get that

$$\begin{aligned} |b|_p &= |x^3 + ax|_p \leq \max\{1, |a|_p\}, \\ |a|_p &= |ax|_p = |b - x^3|_p \leq \max\{1, |b|_p\}, \\ 1 &= |x^3|_p = |b - ax|_p \leq \max\{|a|_p, |b|_p\}. \end{aligned}$$

Thus, if $|a|_p \neq |b|_p$ then $\max\{|a|_p, |b|_p\} = 1$ and if $|a|_p = |b|_p$ then $|a|_p = |b|_p \geq 1$. This yields the claim. \square

We are going to state the solvability criterion for the depressed cubic equation (1.3) in domains \mathbb{Z}_p^* , \mathbb{Z}_p , \mathbb{Q}_p for $p > 3$.

Let $a, b \in \mathbb{Q}_p$ be two nonzero p -adic numbers with $a = \frac{a^*}{|a|_p}$, $b = \frac{b^*}{|b|_p}$ where $a^*, b^* \in \mathbb{Z}_p^*$ with $a^* = a_0 + a_1 \cdot p + a_2 \cdot p^2 + \dots$ and $b^* = b_0 + b_1 \cdot p + b_2 \cdot p^2 + \dots$.

We set $D_0 = -4a_0^3 - 27b_0^2$ and $u_{n+3} = b_0u_n - a_0u_{n+1}$ with $u_1 = 0$, $u_2 = -a_0$, and $u_3 = b_0$ for $n = \overline{1, p-3}$

Theorem 3.2. *Let $p > 3$ be a prime. Then the following statements hold true:*

I *The equation (1.3) has a solution in \mathbb{Z}_p^* if and only if one of the following conditions holds true:*

- I.1 $|a|_p < |b|_p = 1$ and $b_0^{\frac{p-1}{(3,p-1)}} \equiv 1 \pmod{p}$;
- I.2 $|b|_p < |a|_p = 1$ and $(-a_0)^{\frac{p-1}{2}} \equiv 1 \pmod{p}$;
- I.3 $|a|_p = |b|_p = 1$ and $D_0u_{p-2}^2 \not\equiv 9a_0^2 \pmod{p}$;
- I.4 $|a|_p = |b|_p > 1$.

II *The equation (1.3) has a solution in \mathbb{Z}_p if and only if one of the following conditions holds true:*

- II.1 $|a|_p^3 < |b|_p^2 \leq 1$, $3 \mid \log_p |b|_p$, and $b_0^{\frac{p-1}{(3,p-1)}} \equiv 1 \pmod{p}$;
- II.2 $|a|_p^3 = |b|_p^2 \leq 1$ and $D_0u_{p-2}^2 \not\equiv 9a_0^2 \pmod{p}$;
- II.3 $|a|_p^3 > |b|_p^2$ and $|a|_p \geq |b|_p$.

III The equation (1.3) has a solution in \mathbb{Q}_p if and only if one of the following conditions holds true:

- III.1 $|a|_p^3 < |b|_p^2$, $3 \mid \log_p |b|_p$, and $b_0^{\frac{p-1}{(3,p-1)}} \equiv 1 \pmod{p}$;
- III.2 $|a|_p^3 = |b|_p^2$ and $D_0 u_{p-2}^2 \not\equiv 9a_0^2 \pmod{p}$;
- III.3 $|a|_p^3 > |b|_p^2$.

Proof. I. Let $p > 3$ be a prime number and $a, b \in \mathbb{Q}_p$ be two nonzero p -adic numbers. Due to Proposition 3.1, if the equation (1.3) has a solution in \mathbb{Z}_p^* then one of the following assertions holds true: (i) $|a|_p < 1$, $|b|_p = 1$; or (ii) $|a|_p = 1$, $|b|_p < 1$; or (iii) $|a|_p = |b|_p \geq 1$. Let us study every case.

I.1. Now, we want to show that if the equation (1.3) has a solution in \mathbb{Z}_p^* then under the condition $|a|_p < 1$, $|b|_p = 1$ one has that $b_0^{\frac{p-1}{(3,p-1)}} \equiv 1 \pmod{p}$. In fact, let $x \in \mathbb{Z}_p^*$ be a solution of the equation (1.3). Since $|a|_p < 1$ and $|b|_p = 1$, we get that

$$x_0^3 + ax_0 \equiv x_0^3 \equiv b_0 \pmod{p}.$$

Due to Proposition 2.2, this yields that $b_0^{\frac{p-1}{(3,p-1)}} \equiv 1 \pmod{p}$.

Now, we are going to prove that if $|a|_p < 1$, $|b|_p = 1$, and $b_0^{\frac{p-1}{(3,p-1)}} \equiv 1 \pmod{p}$ then the equation (1.3) has a solution in \mathbb{Z}_p^* . In fact, since $b_0^{\frac{p-1}{(3,p-1)}} \equiv 1 \pmod{p}$ there is $x_0 \in \mathbb{Z}$ such that $x_0^3 \equiv b_0 \pmod{p}$ and $(x_0, p) = 1$. Let us consider the following polynomial $f(x) = x^3 + ax - b$. Since $|a|_p < 1$, it is clear that

$$f(x_0) = x_0^3 + ax_0 - b \equiv x_0^3 - b_0 \equiv 0 \pmod{p}, \quad f'(x_0) = 3x_0^2 + a \not\equiv 0 \pmod{p}.$$

Due to Hensel's Lemma 2.1 the equation (1.3) has a solution $x \in \mathbb{Z}_p$ with $|x - x_0|_p \leq \frac{1}{p}$ where $|x_0|_p = 1$. This means that $|x|_p = 1$, i.e., $x \in \mathbb{Z}_p^*$.

I.2. Let us show that if the equation (1.3) has a solution in \mathbb{Z}_p^* then under the condition $|a|_p = 1$, $|b|_p < 1$ one has that $(-a_0)^{\frac{p-1}{2}} \equiv 1 \pmod{p}$. In fact, suppose $x \in \mathbb{Z}_p^*$ is a solution of the equation (1.3). Since $|a|_p = 1$ and $|b|_p < 1$ we get that

$$x_0^3 + a_0 x_0 \equiv x_0(x_0^2 + a_0) \equiv b \equiv 0 \pmod{p}.$$

This means that $x_0^2 + a_0 \equiv 0 \pmod{p}$ and due to Proposition 2.2 we have that $(-a_0)^{\frac{p-1}{2}} \equiv 1 \pmod{p}$.

Now, we want to prove that if $|a|_p = 1$, $|b|_p < 1$, and $(-a_0)^{\frac{p-1}{2}} \equiv 1 \pmod{p}$ then the equation (1.3) has a solution in \mathbb{Z}_p^* . In fact, since $(-a_0)^{\frac{p-1}{2}} \equiv 1 \pmod{p}$ there is $x_0 \in \mathbb{Z}$ such that $x_0^2 + a_0 \equiv 0 \pmod{p}$ and $(x_0, p) = 1$. Let us consider the following polynomial $f(x) = x^3 + ax - b$. Since $|b|_p < 1$, it is clear that

$$\begin{aligned} f(x_0) &= x_0^3 + ax_0 - b \equiv x_0(x_0^2 + a_0) \equiv 0 \pmod{p}, \\ f'(x_0) &= 3x_0^2 + a \equiv 3(x_0^2 + a_0) - 2a_0 \not\equiv 0 \pmod{p}. \end{aligned}$$

Due to Hensel's Lemma 2.1 the equation (1.3) has a solution $x \in \mathbb{Z}_p$ with $|x - x_0|_p \leq \frac{1}{p}$ where $|x_0|_p = 1$. This yields that $|x|_p = 1$, i.e., $x \in \mathbb{Z}_p^*$.

I.3. We are going to show that if the equation (1.3) has a solution in \mathbb{Z}_p^* then under the condition $|a|_p = 1$, $|b|_p = 1$ we have that $D_0 u_{p-2}^2 \not\equiv 9a_0^2 \pmod{p}$. In fact,

let $x \in \mathbb{Z}_p^*$ be a solution of the equation (1.3). Since $|a|_p = 1$ and $|b|_p = 1$ we get that

$$x_0^3 + a_0 x_0 \equiv b_0 \pmod{p}.$$

This means that the depressed cubic equation $x^3 + a_0 x = b_0$ has at least one solution in the finite field \mathbb{F}_p . Due to Proposition 2.4 we have that $D_0 u_{p-2}^2 \not\equiv 9a_0^2 \pmod{p}$.

Now, we are going to prove that if $|a|_p = 1$, $|b|_p = 1$, and $D_0 u_{p-2}^2 \not\equiv 9a_0^2 \pmod{p}$ then the equation (1.3) has a solution in \mathbb{Z}_p^* . Since $D_0 u_{p-2}^2 \not\equiv 9a_0^2 \pmod{p}$, the equation $x^3 + a_0 x \equiv b_0 \pmod{p}$ has at least one solution. Due to Proposition 2.5, among all solutions of the equation $x^3 + a_0 x \equiv b_0 \pmod{p}$, there always exists at least one solution x_0 such that $3x_0^2 + a_0 \not\equiv 0 \pmod{p}$ and $(x_0, p) = 1$.

Again, if we apply Hensel's Lemma 2.1 to the polynomial $f(x) = x^3 + ax - b$ at the point $x = x_0$ then we get that the equation (1.3) has a solution $x \in \mathbb{Z}_p$ with $|x - x_0|_p \leq \frac{1}{p}$ where $|x_0|_p = 1$. This yields that $|x|_p = 1$, i.e., $x \in \mathbb{Z}_p^*$.

I.4. Now, we want to prove that if $|a|_p = |b|_p > 1$ then the equation (1.3) has a solution in \mathbb{Z}_p^* . Let $|a|_p = |b|_p = p^m$, where $m \geq 1$. Then $a = p^{-m}a^*$, $b = p^{-m}b^*$ with $a^*, b^* \in \mathbb{Z}_p^*$. It is clear that the depressed equation $x^3 + p^{-m}a^*x = p^{-m}b^*$ has a solution in \mathbb{Z}_p^* if and only if the equation $p^m x^3 + a^*x = b^*$ has a solution in \mathbb{Z}_p^* , where $a^*, b^* \in \mathbb{Z}_p^*$. To this end, we consider the following polynomial $f(x) = p^m x^3 + a^*x - b^*$. If a_0, b_0 are the first digits of $a^*, b^* \in \mathbb{Z}_p^*$ then there is $x_0 \in \mathbb{Z}$ such that $a_0 x_0 \equiv b_0 \pmod{p}$ and $(x_0, p) = 1$. Then, we obtain that

$$f(x_0) \equiv p^m x_0^3 + a_0 x_0 - b_0 \equiv 0 \pmod{p}, \quad f'(x_0) \equiv 3p^m x_0^2 + a_0 \not\equiv 0 \pmod{p}.$$

Again, due to Hensel's Lemma 2.1, the equation $p^m x^3 + a^*x = b^*$ has a solution $x \in \mathbb{Z}_p^*$ with $|x - x_0|_p \leq \frac{1}{p}$ where $|x_0|_p = 1$. This yields that $x \in \mathbb{Z}_p^*$.

II. Let $p > 3$ be a prime number and $a, b \in \mathbb{Q}_p$ be two nonzero p -adic numbers. Now, we want to provide the solvability criterion for the depressed equation (1.3) in the domain \mathbb{Z}_p .

We know that any p -adic integer x has the following unique form $x = p^k x^*$, where $x^* \in \mathbb{Z}_p^*$ and $k \in \mathbb{N} \cup \{0\}$. Then the depressed equation (1.3) has a solution in \mathbb{Z}_p if and only if there is a nonnegative integer k such that the following equation

$$x^3 + Ax = B \tag{3.1}$$

has a solution in \mathbb{Z}_p^* where $A = p^{-2k}a$, $B = p^{-3k}b$.

Due to the case I, in general, the equation (3.1) has a solution in \mathbb{Z}_p^* if and only if one of the following conditions holds true:

- (i) $|A|_p < |B|_p = 1$, and $b_0^{\frac{p-1}{3(p-1)}} \equiv 1 \pmod{p}$;
- (ii) $|B|_p < |A|_p = 1$, and $(-a_0)^{\frac{p-1}{2}} \equiv 1 \pmod{p}$;
- (iii) $|A|_p = |B|_p = 1$, and $D_0 u_{p-2}^2 \not\equiv 9a_0^2 \pmod{p}$;
- (iv) $|A|_p = |B|_p > 1$.

where $A = p^{-2k} \frac{a^*}{|a|_p}$, $B = p^{-3k} \frac{b^*}{|b|_p}$, and $a^*, b^* \in \mathbb{Z}_p^*$ with

$$a^* = a_0 + a_1 \cdot p + a_2 \cdot p^2 + \cdots; \quad b^* = b_0 + b_1 \cdot p + b_2 \cdot p^2 + \cdots.$$

It is clear that $|A|_p = p^{2k}|a|_p$, $|B|_p = p^{3k}|b|_p$. Now, in every case (i)-(iv), we want to describe all p -adic numbers $a, b \in \mathbb{Q}_p$ for which the equation (3.1) has a solution in \mathbb{Z}_p^* for some nonnegative integer k .

II.1. Suppose that $|A|_p < |B|_p = 1$ and $b_0^{\frac{p-1}{(3,p-1)}} \equiv 1 \pmod{p}$. Since $|B|_p = p^{3k}|b|_p$, we get from $|B|_p = 1$ that $3k = -\log_p |b|_p$. The last equation has a nonnegative integer solution w.r.t k if and only if $\log_p |b|_p$ is divisible by 3 and $|b|_p \leq 1$. Therefore, if $k = -\frac{\log_p |b|_p}{3}$ then it follows from $|A|_p = p^{2k}|a|_p < 1$ that $|a|_p^3 < |b|_p^2$. Consequently, if $|a|_p^3 < |b|_p^2 \leq 1$, $b_0^{\frac{p-1}{(3,p-1)}} \equiv 1 \pmod{p}$ and $3 \mid \log_p |b|_p$ then the equation (3.1) has a solution in \mathbb{Z}_p^* for $k = -\frac{\log_p |b|_p}{3}$.

II.2. Assume that $|A|_p = |B|_p = 1$ and $D_0 u_{p-2}^2 \not\equiv 9a_0^2 \pmod{p}$. Since $|A|_p = p^{2k}|a|_p$, $|B|_p = p^{3k}|b|_p$ we have that $2k = -\log_p |a|_p$ and $3k = -\log_p |b|_p$. The last two equations have a nonnegative integer solution w.r.t k if and only if $\log_p |a|_p$ is divisible by 2, $\log_p |b|_p$ is divisible by 3, and $|a|_p \leq 1$, $|b|_p \leq 1$. Therefore, if $k = -\frac{\log_p |a|_p}{2} = -\frac{\log_p |b|_p}{3}$ then we have that $|a|_p^3 = |b|_p^2$. Consequently, if $|a|_p^3 = |b|_p^2 \leq 1$ and $D_0 u_{p-2}^2 \not\equiv 9a_0^2 \pmod{p}$ then the equation (3.1) has a solution in \mathbb{Z}_p^* for $k = -\frac{\log_p |a|_p}{2} = -\frac{\log_p |b|_p}{3}$.

II.3. We are going to consider the cases $|B|_p < |A|_p = 1$, $(-a_0)^{\frac{p-1}{2}} \equiv 1 \pmod{p}$ and $|A|_p = |B|_p > 1$. Let us study every case.

Let $|B|_p < |A|_p = 1$ and $(-a_0)^{\frac{p-1}{2}} \equiv 1 \pmod{p}$. Since $|A|_p = p^{2k}|a|_p$ we get from $|A|_p = 1$ that $2k = -\log_p |a|_p$. The last equation has a nonnegative integer solution w.r.t k if and only if $\log_p |a|_p$ is even and $|a|_p \leq 1$. Therefore, if $k = -\frac{\log_p |a|_p}{2}$ then it follows from $|B|_p = p^{3k}|b|_p < 1$ that $|a|_p^3 > |b|_p^2$. Consequently, if $|b|_p^2 < |a|_p^3 \leq 1$, $\log_p |a|_p$ is even, and $(-a_0)^{\frac{p-1}{2}} \equiv 1 \pmod{p}$ then the equation (3.1) has a solution in \mathbb{Z}_p^* for $k = -\frac{\log_p |a|_p}{2}$.

Let $|A|_p = |B|_p > 1$. Since $|A|_p = p^{2k}|a|_p$, $|B|_p = p^{3k}|b|_p$ we obtain from $|A|_p = |B|_p$ that $k = \log_p |a|_p - \log_p |b|_p$. Hence, k is a nonnegative integer if and only if $|a|_p \geq |b|_p$. Therefore, if $k = \log_p |a|_p - \log_p |b|_p$ then it follows from $|A|_p = |B|_p > 1$ that $|a|_p^3 > |b|_p^2$. Consequently, if $|a|_p^3 > |b|_p^2$ and $|a|_p \geq |b|_p$ then the equation (3.1) has a solution in \mathbb{Z}_p^* for $k = \log_p |a|_p - \log_p |b|_p$.

It is worth mentioning that if p -adic numbers $a, b \in \mathbb{Q}_p$ satisfy the conditions $|b|_p^2 < |a|_p^3 \leq 1$, $\log_p |a|_p$ is even, and $(-a_0)^{\frac{p-1}{2}} \equiv 1 \pmod{p}$ then they satisfy the conditions $|a|_p^3 > |b|_p^2$ and $|a|_p \geq |b|_p$ as well. Consequently, regardless of whether p -adic numbers $a, b \in \mathbb{Q}_p$ satisfy the conditions $|b|_p^2 < |a|_p^3 \leq 1$, $\log_p |a|_p$ is even, and $(-a_0)^{\frac{p-1}{2}} \equiv 1 \pmod{p}$, the equation (3.1) has a solution in \mathbb{Z}_p^* if $|a|_p^3 > |b|_p^2$ and $|a|_p \geq |b|_p$. Moreover, if $|b|_p^2 < |a|_p^3 \leq 1$, $\log_p |a|_p$ is even, and $(-a_0)^{\frac{p-1}{2}} \equiv 1 \pmod{p}$ then the equation (3.1) has at least two distinct solutions in \mathbb{Z}_p^* for two distinct nonnegative integers $k = -\frac{\log_p |a|_p}{2}$ and $k = \log_p |a|_p - \log_p |b|_p$, otherwise the equation (3.1) has at least one solution in \mathbb{Z}_p^* for $k = \log_p |a|_p - \log_p |b|_p$.

III. Let $p > 3$ be a prime number and $a, b \in \mathbb{Q}_p$ be two nonzero p -adic numbers. In order to provide the solvability criterion for the depressed equation (1.3) in the domain \mathbb{Q}_p , we apply the same method that one used in the case II, but with the assumption that k is any integer number. This completes the proof. \square

4. THE NUMBER OF SOLUTIONS IN DOMAINS \mathbb{Z}_p^* , \mathbb{Z}_p , \mathbb{Q}_p , WITH $p > 3$

In this section, we are aiming to describe the numbers $\mathbf{N}_{\mathbb{Z}_p^*}(x^3 + ax - b)$, $\mathbf{N}_{\mathbb{Z}_p}(x^3 + ax - b)$, and $\mathbf{N}_{\mathbb{Q}_p}(x^3 + ax - b)$ of solutions of the depressed cubic equation (1.3) in domains \mathbb{Z}_p^* , \mathbb{Z}_p , and \mathbb{Q}_p , respectively, whenever $p > 3$ and $ab \neq 0$.

Let $a, b \in \mathbb{Q}_p$ be two nonzero p -adic numbers with $a = \frac{a^*}{|a|_p}$, $b = \frac{b^*}{|b|_p}$ where $a^*, b^* \in \mathbb{Z}_p^*$ with $a^* = a_0 + a_1 \cdot p + a_2 \cdot p^2 + \dots$ and $b^* = b_0 + b_1 \cdot p + b_2 \cdot p^2 + \dots$.

We set $D_0 = -4a_0^3 - 27b_0^2$ and $u_{n+3} = b_0u_n - a_0u_{n+1}$ with $u_1 = 0$, $u_2 = -a_0$, and $u_3 = b_0$ for $n = \overline{1, p-3}$.

Let $D = -4(a|a|_p)^3 - 27(b|b|_p)^2$. We have $D = \frac{D^*}{|D|_p}$ whenever $D \neq 0$, where $D^* \in \mathbb{Z}_p^*$ and $D^* = d_0 + d_1 \cdot p + d_2 \cdot p^2 + \dots$.

Theorem 4.1. *Let $p > 3$ be a prime. Then the following statements hold true:*

$$\mathbf{N}_{\mathbb{Z}_p^*}(x^3 + ax - b) = \begin{cases} 3, & |a|_p < |b|_p = 1, \ p \equiv 1 \pmod{3}, \ b_0^{\frac{p-1}{3}} \equiv 1 \pmod{p} \\ 3, & |a|_p = |b|_p = 1, \ D = 0 \\ 3, & |a|_p = |b|_p = 1, \ 0 < |D|_p < 1, \ 2 \mid \log_p |D|_p, \ d_0^{\frac{p-1}{2}} \equiv 1 \pmod{p} \\ 3, & |a|_p = |b|_p = 1, \ |D|_p = 1, \ u_{p-2} \equiv 0 \pmod{p} \\ 2, & |b|_p < |a|_p = 1, \ (-a_0)^{\frac{p-1}{2}} \equiv 1 \pmod{p} \\ 1, & |a|_p < |b|_p = 1, \ p \equiv 2 \pmod{3} \\ 1, & |a|_p = |b|_p = 1, \ 0 < |D|_p < 1, \ 2 \mid \log_p |D|_p, \ d_0^{\frac{p-1}{2}} \not\equiv 1 \pmod{p} \\ 1, & |a|_p = |b|_p = 1, \ 0 < |D|_p < 1, \ 2 \nmid \log_p |D|_p, \\ 1, & |a|_p = |b|_p = 1, \ D_0 u_{p-2}^2 \not\equiv 0, 9a_0^2 \pmod{p} \\ 1, & |a|_p = |b|_p > 1 \\ 0, & \text{otherwise} \end{cases}$$

$$\mathbf{N}_{\mathbb{Z}_p}(x^3 + ax - b) = \begin{cases} 3, & |a|_p^3 < |b|_p^2 \leq 1, \ 3 \mid \log_p |b|_p, \ p \equiv 1 \pmod{3}, \ b_0^{\frac{p-1}{3}} \equiv 1 \pmod{p} \\ 3, & |a|_p^3 = |b|_p^2 \leq 1, \ D = 0 \\ 3, & |a|_p^3 = |b|_p^2 \leq 1, \ 0 < |D|_p < 1, \ 2 \mid \log_p |D|_p, \ d_0^{\frac{p-1}{2}} \equiv 1 \pmod{p} \\ 3, & |a|_p^3 = |b|_p^2 \leq 1, \ |D|_p = 1, \ u_{p-2} \equiv 0 \pmod{p} \\ 3, & |b|_p^2 < |a|_p^3 \leq 1, \ 2 \mid \log_p |a|_p, \ (-a_0)^{\frac{p-1}{2}} \equiv 1 \pmod{p} \\ 1, & |a|_p^3 < |b|_p^2 \leq 1, \ 3 \mid \log_p |b|_p, \ p \equiv 2 \pmod{3} \\ 1, & |a|_p^3 = |b|_p^2 \leq 1, \ 0 < |D|_p < 1, \ 2 \mid \log_p |D|_p, \ d_0^{\frac{p-1}{2}} \not\equiv 1 \pmod{p} \\ 1, & |a|_p^3 = |b|_p^2 \leq 1, \ 0 < |D|_p < 1, \ 2 \nmid \log_p |D|_p, \\ 1, & |a|_p^3 = |b|_p^2 \leq 1, \ D_0 u_{p-2}^2 \not\equiv 0, 9a_0^2 \pmod{p} \\ 1, & |b|_p^2 < |a|_p^3 \leq 1, \ 2 \mid \log_p |a|_p, \ (-a_0)^{\frac{p-1}{2}} \not\equiv 1 \pmod{p} \\ 1, & |b|_p^2 < |a|_p^3 \leq 1, \ 2 \nmid \log_p |a|_p \\ 1, & |b|_p^2 < |a|_p^3, \ |b|_p \leq |a|_p, \ |a|_p > 1 \\ 0, & \text{otherwise} \end{cases}$$

$$\mathbf{N}_{\mathbb{Q}_p}(x^3+ax-b) = \begin{cases} 3, & |a|_p^3 < |b|_p^2, \ 3 \mid \log_p |b|_p, \ p \equiv 1 \pmod{3}, \ b_0^{\frac{p-1}{3}} \equiv 1 \pmod{p} \\ 3, & |a|_p^3 = |b|_p^2, \ D = 0 \\ 3, & |a|_p^3 = |b|_p^2, \ 0 < |D|_p < 1, \ 2 \mid \log_p |D|_p, \ d_0^{\frac{p-1}{2}} \equiv 1 \pmod{p} \\ 3, & |a|_p^3 = |b|_p^2, \ |D|_p = 1, \ u_{p-2} \equiv 0 \pmod{p} \\ 3, & |a|_p^3 > |b|_p^2, \ 2 \mid \log_p |a|_p, \ (-a_0)^{\frac{p-1}{2}} \equiv 1 \pmod{p} \\ 1, & |a|_p^3 < |b|_p^2, \ 3 \mid \log_p |b|_p, \ p \equiv 2 \pmod{3} \\ 1, & |a|_p^3 = |b|_p^2, \ 0 < |D|_p < 1, \ 2 \mid \log_p |D|_p, \ d_0^{\frac{p-1}{2}} \not\equiv 1 \pmod{p} \\ 1, & |a|_p^3 = |b|_p^2, \ 0 < |D|_p < 1, \ 2 \nmid \log_p |D|_p, \\ 1, & |a|_p^3 = |b|_p^2, \ D_0 u_{p-2}^2 \not\equiv 0, 9a_0^2 \pmod{p} \\ 1, & |a|_p^3 > |b|_p^2, \ 2 \mid \log_p |a|_p, \ (-a_0)^{\frac{p-1}{2}} \not\equiv 1 \pmod{p} \\ 1, & |a|_p^3 > |b|_p^2, \ 2 \nmid \log_p |a|_p \\ 0, & \text{otherwise} \end{cases}$$

Proof. Let $p > 3$ be a prime number and $a, b \in \mathbb{Q}_p$ be two nonzero p -adic numbers.

CASE \mathbb{Z}_p^* : We want to describe the number $\mathbf{N}_{\mathbb{Z}_p^*}(x^3 + ax - b)$ of solutions of the depressed cubic equation (1.3) in the domain \mathbb{Z}_p^* .

Due to the case I of Theorem 3.2, the depressed cubic equation (1.3) has a solution in \mathbb{Z}_p^* if and only if one of conditions I.1-I.4 holds true. We want to find the number of solutions in every case.

Let us consider the case I.1, i.e., $|a|_p < |b|_p = 1$ and $b_0^{\frac{p-1}{(3,p-1)}} \equiv 1 \pmod{p}$. In this case, due to Hensel's Lemma 2.1 as we showed in the proof of I.1, the number of solutions of the equation (1.3) in \mathbb{Z}_p^* is the same as the number of solutions of the equation $x_0^3 = b_0$ in \mathbb{F}_p . Then, due to Proposition 2.2, the last equation has 3 distinct solutions if $p \equiv 1 \pmod{3}$ and it has a unique solution if $p \equiv 2 \pmod{3}$.

Therefore, if $|a|_p < |b|_p = 1$, $p \equiv 1 \pmod{3}$, and $b_0^{\frac{p-1}{3}} \equiv 1 \pmod{p}$ then the equation (1.3) has 3 distinct solutions in \mathbb{Z}_p^* and if $|a|_p < |b|_p = 1$, $p \equiv 2 \pmod{3}$ and $b_0^{p-1} \equiv 1 \pmod{p}$ then the equation (1.3) has a unique solution in \mathbb{Z}_p^* . It is worth mentioning that one always has $b_0^{p-1} \equiv 1 \pmod{p}$ since $(b_0, p) = 1$.

Let us consider the case I.2, i.e., $|b|_p < |a|_p = 1$ and $(-a_0)^{\frac{p-1}{2}} \equiv 1 \pmod{p}$. In this case, due to Hensel's Lemma 2.1 as we showed in the proof of I.2, the number of solutions of the equation (1.3) in \mathbb{Z}_p^* is the same as the number of solutions of the equation $x_0^2 = -a_0$ in \mathbb{F}_p . Since $(-a_0)^{\frac{p-1}{2}} \equiv 1 \pmod{p}$, the last equation has 2 distinct solutions in \mathbb{F}_p .

Therefore, if $|b|_p < |a|_p = 1$ and $(-a_0)^{\frac{p-1}{2}} \equiv 1 \pmod{p}$ then the depressed cubic equation (1.3) has 2 distinct solutions in \mathbb{Z}_p^* .

Let us consider the case I.3, i.e., $|a|_p = |b|_p = 1$ and $D_0 u_{p-2}^2 \not\equiv 9a_0^2 \pmod{p}$. In this case, as we showed in the proof of I.3, the equation (1.3) has a solution \bar{x} such that $\bar{x} \equiv \bar{x}_0 \pmod{p}$, where \bar{x}_0 is a solution of the following congruent equation

$$x_0^3 + a_0 x_0 \equiv b_0 \pmod{p} \quad (4.1)$$

such that $3\bar{x}_0^2 + a_0 \not\equiv 0 \pmod{p}$.

Due to Proposition 2.4, if $D_0 u_{p-2}^2 \not\equiv 0, 9a_0^2 \pmod{p}$ then the equation (4.1) does not have any solution except \bar{x}_0 . Therefore, due to Hensel's Lemma 2.1, if $|a|_p = |b|_p = 1$ and $D_0 u_{p-2}^2 \not\equiv 0, 9a_0^2 \pmod{p}$ then the equation (1.3) has a unique solution in \mathbb{Z}_p^* .

Now, let us study the case $|a|_p = |b|_p = 1$ and $D_0 u_{p-2}^2 \equiv 0 \pmod{p}$. In this case, due to Proposition 2.4, the congruent equation (4.1) has 2 more solutions besides \bar{x}_0 . We denote them by x_0 and y_0 . There is no loss of generality in assuming that $0 < x_0, y_0 < p$.

Due to Proposition 2.5, if $D_0 \not\equiv 0 \pmod{p}$ then all solutions x_0, y_0, \bar{x}_0 of the congruent equation (4.1) are distinct from each other and $3x_0^2 + a_0 \not\equiv 0 \pmod{p}$, $3y_0^2 + a_0 \not\equiv 0 \pmod{p}$. Therefore, due to Hensel's Lemma 2.1, the equation (1.3) has 2 more solutions x, y besides \bar{x} such that $x \equiv x_0 \pmod{p}$, $y \equiv y_0 \pmod{p}$. Hence, $|a|_p = |b|_p = 1$, $D_0 \not\equiv 0 \pmod{p}$ (equivalently $|D|_p = 1$) and $u_{p-2} \equiv 0 \pmod{p}$ then the equation (1.3) has 3 distinct solutions in \mathbb{Z}_p^* .

Again according to Proposition 2.5, if $D_0 \equiv 0 \pmod{p}$ then two solutions x_0, y_0 of the congruent equation (4.1) are equal to each other and $\bar{x}_0 = -2x_0$, $3x_0^2 + a_0 \equiv 0 \pmod{p}$. Now, we are going to study this case in a detail.

Since \bar{x} is a solution of the equation (1.3), one can get that

$$x^3 + ax - b = (x - \bar{x})(x^2 + \bar{x}x + \bar{x}^2 + a).$$

We are going to study the following quadratic equation

$$x^2 + \bar{x}x + \bar{x}^2 + a = 0. \quad (4.2)$$

It is clear that

$$\left(x + \frac{\bar{x}}{2}\right)^2 = -\left(3\left(\frac{\bar{x}}{2}\right)^2 + a\right).$$

Since $a, \bar{x} \in \mathbb{Z}_p^*$ and $p > 3$, we have that $\left|3\left(\frac{\bar{x}}{2}\right)^2 + a\right|_p \leq 1$. Since \bar{x} is a solution of the equation (1.3), one can get that $4\bar{x}\left(3\left(\frac{\bar{x}}{2}\right)^2 + a\right) = a\bar{x} + 3b$. We then have that

$$\begin{aligned} D &= -4a^3 - 27b^2 = 3(a^2\bar{x}^2 - 9b^2) - a^2(3\bar{x}^2 + 4a) \\ &= 12\bar{x}\left(3\left(\frac{\bar{x}}{2}\right)^2 + a\right)(a\bar{x} - 3b) - 4a^2\left(3\left(\frac{\bar{x}}{2}\right)^2 + a\right) \\ &= 4\left(3\left(\frac{\bar{x}}{2}\right)^2 + a\right)(3a\bar{x}^2 - 9b\bar{x} - a^2). \end{aligned}$$

Since $\bar{x} \equiv \bar{x}_0 = -2x_0 \pmod{p}$, $3x_0^2 + a_0 \equiv 0 \pmod{p}$, and $2x_0a_0 \equiv 3b_0 \pmod{p}$ we get that $3a\bar{x}^2 - 9b\bar{x} - a^2 \equiv -9a_0^2 \pmod{p}$. This means that $|3a\bar{x}^2 - 9b\bar{x} - a^2|_p = 1$ and $-(3a\bar{x}^2 - 9b\bar{x} - a^2)$ is a complete square of some p -adic integer number. Therefore, we obtain that

$$-\left(3\left(\frac{\bar{x}}{2}\right)^2 + a\right) = \frac{D}{-4(3a\bar{x}^2 - 9b\bar{x} - a^2)} \quad (4.3)$$

Let us analyze the quadratic equation (4.2).

If $D = 0$ then the quadratic equation (4.2) has solutions $x_1 = x_2 = \frac{3b}{2a}$ in \mathbb{Z}_p^* . Therefore, $|a|_p = |b|_p = 1$ and $D = 0$ then the cubic equation (1.3) has 3 solutions such that $x_1 = x_2 = \frac{3b}{2a}$ and $x_3 = -\frac{3b}{a}$.

Let $D \neq 0$. Since $D \equiv D_0 \equiv 0 \pmod{p}$, there exists $k \in \mathbb{N}$ such that $|D|_p = p^{-k}$, i.e., $D = \frac{D^*}{|D|_p}$, where $D^* \in \mathbb{Z}_p^*$ with $D^* = d_0 + d_1 \cdot p + d_2 \cdot p^2 + \dots$.

The quadratic equation (4.2) has a solution if and only if $\log_p |D|_p = -k$ is even number and $d_0^{\frac{p-1}{2}} \equiv 1 \pmod{p}$. In this case $- \left(3 \left(\frac{\bar{x}}{2} \right)^2 + a \right)$ is a complete square and the quadratic equation (4.2) has two distinct solutions in \mathbb{Z}_p^* as follows

$$x_{\pm} = -\frac{\bar{x}}{2} \pm \sqrt{- \left(3 \left(\frac{\bar{x}}{2} \right)^2 + a \right)} \quad (4.4)$$

Therefore, if $|a|_p = |b|_p = 1$, $0 < |D|_p < 1$, $2 \mid \log_p |D|_p$, and $d_0^{\frac{p-1}{2}} \equiv 1 \pmod{p}$ then the cubic equation (1.3) has 3 distinct solutions in \mathbb{Z}_p^* . If $|a|_p = |b|_p = 1$, $0 < |D|_p < 1$, $2 \mid \log_p |D|_p$, and $d_0^{\frac{p-1}{2}} \not\equiv 1 \pmod{p}$ or $|a|_p = |b|_p = 1$, $0 < |D|_p < 1$, and $2 \nmid \log_p |D|_p$ then the cubic equation (1.3) has a unique solutions in \mathbb{Z}_p^* .

Let us consider the case I.4, i.e., $|a|_p = |b|_p > 1$. In this case, due to Hensel's Lemma 2.1 as we showed in the proof of I.4, the number of solutions of the equation (1.3) in \mathbb{Z}_p^* is the same as the number of solutions of the linear equation $a_0 x_0 = b_0$ in \mathbb{F}_p . Since $a_0 \neq 0$, the last equation has a unique solution. Therefore, if $|a|_p = |b|_p > 1$ then the depressed cubic equation (1.3) has a unique solution in \mathbb{Z}_p^* .

CASE \mathbb{Z}_p : We shall study the number $\mathbf{N}_{\mathbb{Z}_p}(x^3 + ax - b)$ of solutions of the cubic equation (1.3) in the domain \mathbb{Z}_p .

Due to the case II of Theorem 3.2, the cubic equation (1.3) has a solution in \mathbb{Z}_p if and only if one of conditions II.1-II.3 holds true. We want to find the number of solutions in every case.

Let us consider the case II.1, i.e., $|a|_p^3 < |b|_p^2 \leq 1$, $3 \mid \log_p |b|_p$, and $b_0^{\frac{p-1}{(3,p-1)}} \equiv 1 \pmod{p}$. In this case, as we showed in the proof of II.1, the number of solutions of the cubic equation (1.3) in the domain \mathbb{Z}_p is the same as the number of solutions of the following equation in the domain \mathbb{Z}_p^* :

$$y^3 + a \sqrt[3]{|b|_p^2} y = b^*. \quad (4.5)$$

Then it is clear that $\left| a \sqrt[3]{|b|_p^2} \right|_p < |b^*|_p = 1$ and $b_0^{\frac{p-1}{(3,p-1)}} \equiv 1 \pmod{p}$. In this case, as we already discussed that if $p \equiv 1 \pmod{3}$ then the equation (4.5) has 3 distinct solutions in \mathbb{Z}_p^* and if $p \equiv 2 \pmod{3}$ then the equation (4.5) has a unique solution in \mathbb{Z}_p^* .

Consequently, if $|a|_p^3 < |b|_p^2 \leq 1$, $3 \mid \log_p |b|_p$, $p \equiv 1 \pmod{3}$, and $b_0^{\frac{p-1}{3}} \equiv 1 \pmod{p}$ then the cubic equation (1.3) has 3 distinct solutions in \mathbb{Z}_p and if $|a|_p^3 < |b|_p^2 \leq 1$, $3 \mid \log_p |b|_p$, and $p \equiv 2 \pmod{3}$ then the cubic equation (1.3) has a unique solution in \mathbb{Z}_p .

Let us consider the case II.2, i.e., $|a|_p^3 = |b|_p^2 \leq 1$ and $D_0 u_{p-2}^2 \not\equiv 9a_0^2 \pmod{p}$. In this case, as we showed in the proof of II.2 that the number of solutions of the cubic equation (1.3) in the domain \mathbb{Z}_p is the same as the number of solutions of the following equation in the domain \mathbb{Z}_p^*

$$y^3 + a^* y = b^*. \quad (4.6)$$

Then it is clear that $|a^*|_p = |b^*|_p = 1$ and $D_0 u_{p-2}^2 \not\equiv 9a_0^2 \pmod{p}$.

Let $D = -4(a^*)^3 - 27(b^*)^2$. We have $D = \frac{D^*}{|D|_p}$ whenever $D \neq 0$, where $D^* \in \mathbb{Z}_p^*$ and $D^* = d_0 + d_1 \cdot p + d_2 \cdot p^2 + \dots$.

The number of solutions of the equation (4.6) was studied very well in the case $|a^*|_p = |b^*|_p = 1$ and $D_0 u_{p-2}^2 \not\equiv 9a_0^2 \pmod{p}$. The equation (4.6) has either a unique solution or 3 solutions.

Consequently, the cubic equation (1.3) has 3 solutions if and only if one of the following conditions holds true: (i) $|a|_p^3 = |b|_p^2 \leq 1$ and $D = 0$ or (ii) $|a|_p^3 = |b|_p^2 \leq 1$, $0 < |D|_p < 1$, $2 \mid \log_p |D|_p$, and $d_0^{\frac{p-1}{2}} \equiv 1 \pmod{p}$ or (iii) $|a|_p^3 = |b|_p^2 \leq 1$, $|D|_p = 1$, and $u_{p-2} \equiv 0 \pmod{p}$. The cubic equation (1.3) has a unique solution if and only if one of the following conditions holds true: (i) $|a|_p^3 = |b|_p^2 \leq 1$, $0 < |D|_p < 1$, $2 \nmid \log_p |D|_p$, and $d_0^{\frac{p-1}{2}} \not\equiv 1 \pmod{p}$ or (ii) $|a|_p^3 = |b|_p^2 \leq 1$, $0 < |D|_p < 1$, and $2 \nmid \log_p |D|_p$ or (iii) $|a|_p^3 = |b|_p^2 \leq 1$ and $D_0 u_{p-2}^2 \equiv 0, 9a_0^2 \pmod{p}$.

Let us consider the case II.3, i.e., $|a|_p^3 > |b|_p^2$ and $|a|_p \geq |b|_p$.

One can easily check that

$$\Delta = \Delta_1 \cup \Delta_2 \cup \Delta_3 \cup \Delta_4,$$

where

$$\begin{aligned} \Delta &= \{(a, b) : |a|_p^3 > |b|_p^2, |a|_p \geq |b|_p\}, \\ \Delta_1 &= \{(a, b) : |b|_p^2 < |a|_p^3 \leq 1, 2 \mid \log_p |a|_p, (-a_0)^{\frac{p-1}{2}} \equiv 1 \pmod{p}\}, \\ \Delta_2 &= \{(a, b) : |b|_p^2 < |a|_p^3 \leq 1, 2 \mid \log_p |a|_p, (-a_0)^{\frac{p-1}{2}} \not\equiv 1 \pmod{p}\}, \\ \Delta_3 &= \{(a, b) : |b|_p^2 < |a|_p^3 \leq 1, 2 \nmid \log_p |a|_p\}, \\ \Delta_4 &= \{(a, b) : |a|_p^3 > |b|_p^2, |a|_p \geq |b|_p, |a|_p > 1\}. \end{aligned}$$

In the case Δ_1 , as we showed in the proof of II.3, the number of solutions of the cubic equation (1.3) in the domain \mathbb{Z}_p is the same as the total number of solutions of the following equations in the domain \mathbb{Z}_p^* :

$$y^3 + a^* y = b \sqrt{|a|_p^3}, \quad (4.7)$$

$$z^3 + a \left| \frac{b}{a} \right|_p z = b \left| \frac{b}{a} \right|_p^3, \quad (4.8)$$

It is then clear that $|a^*|_p = 1$, $\left| b \sqrt{|a|_p^3} \right|_p < 1$ and $\left| a \left| \frac{b}{a} \right|_p^2 \right|_p = \left| b \left| \frac{b}{a} \right|_p^3 \right|_p > 1$.

In this case, as we already discussed, the equation (4.7) has 2 distinct solutions in \mathbb{Z}_p^* and the equation (4.8) has a unique solution in \mathbb{Z}_p^* . Consequently, the cubic equation (1.3) has 3 solutions in \mathbb{Z}_p .

In the case $\Delta_2 \cup \Delta_3 \cup \Delta_4$, as we showed in the proof of II.3, the number of solutions of the cubic equation (1.3) in the domain \mathbb{Z}_p is the same as the number of solutions of the equation (4.8) in the domain \mathbb{Z}_p^* . We know that the equation (4.8) has a unique solution in \mathbb{Z}_p^* . Consequently, the cubic equation (1.3) has a unique solution in \mathbb{Z}_p .

CASE \mathbb{Q}_p : Analogously, one can study the number $\mathbf{N}_{\mathbb{Q}_p}(x^3 + ax - b)$ of solutions of the cubic equation (1.3) in the domain \mathbb{Q}_p . This completes the proof. \square

5. A p -ADIC CARDANO FORMULA

As we already mentioned, in general, by means of Cardano's method we could not detect solutions of all cubic equations over the p -adic field. In this section, we shall describe all possible cases in which Cardano's method is applicable to solve the cubic equation in \mathbb{Q}_p .

Let $a, b \in \mathbb{Q}_p$ be two nonzero p -adic numbers with $a = \frac{a^*}{|a|_p}$, $b = \frac{b^*}{|b|_p}$ where $a^*, b^* \in \mathbb{Z}_p^*$ with $a^* = a_0 + a_1 \cdot p + a_2 \cdot p^2 + \dots$ and $b^* = b_0 + b_1 \cdot p + b_2 \cdot p^2 + \dots$.

We set $D_0 = -4a_0^3 - 27b_0^2$ and $u_{n+3} = b_0u_n - a_0u_{n+1}$ with $u_1 = 0$, $u_2 = -a_0$, and $u_3 = b_0$ for $n = 1, p-3$.

Let $D = -4(a|a|_p)^3 - 27(b|b|_p)^2$. We have $D = \frac{D^*}{|D|_p}$ whenever $D \neq 0$, where $D^* \in \mathbb{Z}_p^*$ and $D^* = d_0 + d_1 \cdot p + d_2 \cdot p^2 + \dots$.

Let $\Delta_0 \in \{1, 2, \dots, p-1\}$ such that $\Delta_0^2 \equiv -3d_0 \pmod{p}$ whenever $-3d_0$ is a quadratic residue.

Theorem 5.1. *The Cardano method is applicable for the depressed cubic equation (1.3) in \mathbb{Q}_p and one of solutions has the following form*

$$x = \sqrt[3]{\frac{b}{2} + \sqrt{\left(\frac{a}{3}\right)^3 + \left(\frac{b}{2}\right)^2}} + \sqrt[3]{\frac{b}{2} - \sqrt{\left(\frac{a}{3}\right)^3 + \left(\frac{b}{2}\right)^2}} \quad (5.1)$$

if and only if one of the following conditions holds true:

- I.1 $|a|_p^3 < |b|_p^2$, $3 \mid \log_p |b|_p$, and $b_0^{\frac{p-1}{(3,p-1)}} \equiv 1 \pmod{p}$;
- I.2 $|a|_p^3 = |b|_p^2$, $D = 0$, and $(4b_0)^{\frac{p-1}{(3,p-1)}} \equiv 1 \pmod{p}$;
- I.3 $|a|_p^3 = |b|_p^2$, $0 < |D|_p < 1$, $2 \mid \log_p |D|_p$,
 $(-3d_0)^{\frac{p-1}{2}} \equiv 1 \pmod{p}$, and $(4b_0)^{\frac{p-1}{(3,p-1)}} \equiv 1 \pmod{p}$;
- I.4 $|a|_p^3 = |b|_p^2$, $|D|_p = 1$, $D_0u_{p-2}^2 \not\equiv 9a_0^2 \pmod{p}$,
 $(-3d_0)^{\frac{p-1}{2}} \equiv 1 \pmod{p}$, and $(108b_0 + 12\Delta_0)^{\frac{p-1}{(3,p-1)}} \equiv 1 \pmod{p}$;
- I.5 $|a|_p^3 > |b|_p^2$, $2 \mid \log_p |a|_p$, and $(3a_0)^{\frac{p-1}{2}} \equiv 1 \pmod{p}$

Proof. We want to describe all $a, b \in \mathbb{Q}_p$ in which the expression (5.1) is well defined in \mathbb{Q}_p . Let us consider III case of Theorem 3.2 where the cubic equation has at least one solution.

$$\text{III.1 } |a|_p^3 < |b|_p^2, 3 \mid \log_p |b|_p, \text{ and } b_0^{\frac{p-1}{(3,p-1)}} \equiv 1 \pmod{p}.$$

Now, we show that the expression (5.1) is meaningful in \mathbb{Q}_p . In fact, since $\left| \left(\frac{a}{3} \right)^3 \right|_p < \left| \left(\frac{b}{2} \right)^2 \right|_p$, the expression $\sqrt{\left(\frac{a}{3} \right)^3 + \left(\frac{b}{2} \right)^2}$ is well defined and $\left| \sqrt{\left(\frac{a}{3} \right)^3 + \left(\frac{b}{2} \right)^2} \right|_p = \left| \frac{b}{2} \right|_p = |b|_p$.

Since $3 \mid \log_p |b|_p$, and $b_0^{\frac{p-1}{(3,p-1)}} \equiv 1 \pmod{p}$, the expression $\frac{b}{2} + \sqrt{\left(\frac{a}{3} \right)^3 + \left(\frac{b}{2} \right)^2}$ is a cube of some p -adic number. It means that $\sqrt[3]{\frac{b}{2} + \sqrt{\left(\frac{a}{3} \right)^3 + \left(\frac{b}{2} \right)^2}}$ is meaningful. On the other hand, we have that

$$\left(\frac{b}{2} + \sqrt{\left(\frac{a}{3} \right)^3 + \left(\frac{b}{2} \right)^2} \right) \left(\frac{b}{2} - \sqrt{\left(\frac{a}{3} \right)^3 + \left(\frac{b}{2} \right)^2} \right) = - \left(\frac{a}{3} \right)^3. \quad (5.2)$$

Therefore, the expressions $\sqrt[3]{\frac{b}{2} - \sqrt{\left(\frac{a}{3} \right)^3 + \left(\frac{b}{2} \right)^2}}$ and (5.1) are meaningful.

III.2 $|a|_p^3 = |b|_p^2$ and $D_0 u_{p-2}^2 \not\equiv 9a_0^2 \pmod{p}$;

It is clear that $\left(\frac{a}{3} \right)^3 + \left(\frac{b}{2} \right)^2 = \frac{1}{324|b|_p^2} \cdot (-3D)$. Then the last expression is a perfect square if and only if one of the following conditions holds true:

- (i) $D = 0$;
- (ii) $0 < |D|_p < 1$, $2 \mid \log_p |D|_p$, and $(-3d_0)^{\frac{p-1}{2}} \equiv 1 \pmod{p}$;
- (iii) $|D|_p = 1$ and $(-3d_0)^{\frac{p-1}{2}} \equiv 1 \pmod{p}$.

We shall study every case.

Let $D = 0$. Then the expression (5.1) is meaningful if and only if $\frac{b}{2}$ is a cube of some p -adic number, i.e., $(4b_0)^{\frac{p-1}{(3,p-1)}} \equiv 1 \pmod{p}$.

Let $0 < |D|_p < 1$, $2 \mid \log_p |D|_p$, and $(-3d_0)^{\frac{p-1}{2}} \equiv 1 \pmod{p}$.

In this case, we have that $\left| \frac{b}{2} \right|_p > \left| \sqrt{\left(\frac{a}{3} \right)^3 + \left(\frac{b}{2} \right)^2} \right|_p$. Therefore, the expression (5.1) is meaningful if and only if $\frac{b}{2}$ is a cube of some p -adic number, i.e., $(4b_0)^{\frac{p-1}{(3,p-1)}} \equiv 1 \pmod{p}$.

Let $|D|_p = 1$ and $(-3d_0)^{\frac{p-1}{2}} \equiv 1 \pmod{p}$.

In this case, we obtain that $\left| \frac{b}{2} \right|_p = \left| \sqrt{\left(\frac{a}{3} \right)^3 + \left(\frac{b}{2} \right)^2} \right|_p$. Due to (5.2), we get that

$$\left| \frac{b}{2} \pm \sqrt{\left(\frac{a}{3} \right)^3 + \left(\frac{b}{2} \right)^2} \right|_p = \left| \frac{b}{2} \right|_p.$$

Therefore, the expression (5.1) is meaningful if and only if $(108b_0 + 12\Delta_0)^{\frac{p-1}{(3,p-1)}} \equiv 1 \pmod{p}$, where $\Delta_0 \in \{1, 2, \dots, p-1\}$ such that $\Delta_0^2 \equiv -3d_0 \pmod{p}$.

III.3 $|a|_p^3 > |b|_p^2$.

We know that $\left| \left(\frac{a}{3} \right)^3 \right|_p > \left| \left(\frac{b}{2} \right)^2 \right|_p$. Then, the expression $\sqrt{\left(\frac{a}{3} \right)^3 + \left(\frac{b}{2} \right)^2}$ is well defined if and only if $\frac{a}{3}$ is a perfect square. The last one means that $2 \mid \log_p |a|_p$, and $(3a_0)^{\frac{p-1}{2}} \equiv 1 \pmod{p}$.

In this case, we have that $\left| \left(\sqrt{\frac{a}{3}} \right)^3 \right|_p > \left| \frac{b}{2} \right|_p$. Therefore, the expressions $\frac{b}{2} + \sqrt{\left(\frac{a}{3} \right)^3 + \left(\frac{b}{2} \right)^2}$ and $\frac{b}{2} - \sqrt{\left(\frac{a}{3} \right)^3 + \left(\frac{b}{2} \right)^2}$ are cube of some p -adic numbers. This means that the expression (5.1) is well defined in \mathbb{Q}_p . □

ACKNOWLEDGEMENT

The Author (M.S.) is grateful to Pah Chin Hee for his valued discussion. We are thank Jan Kohlhaase for his attention and some comments on our papers.

REFERENCES

- [1] L.Ya. Arafava, B. Dragovich, P.H. Frampton, I.V. Volovich, Wave function of the universe and p -adic gravity, *Mod. Phys. Lett. A* **6** (1991), 4341–4358.
- [2] T.M. Apostol, *Introduction to Analytic Number Theory*, Springer-Verlag, New York, 1972.
- [3] M. Avendao, A. Ibrahim, J. M. Rojas, K. Rusek, Near NP-Completeness for Detecting p -adic Rational Roots in One Variable, [arXiv:1001.4252](#).
- [4] M. Avendao, A. Ibrahim, J. M. Rojas, K. Rusek, Faster p -adic Feasibility for Certain Multivariate Sparse Polynomials, [arXiv:1010.5310](#).
- [5] E. Beltrametti, G. Cassinelli, Quantum mechanics and p -adic numbers, *Found. Phys.*, **2** (1972), 1–7.
- [6] Z. I. Borevich, I. R. Shafarevich, *Number Theory*, Acad. Press, New York, 1966.
- [7] J.M. Casas, B.A.Omirov, U.A. Rozikov, Solvability criteria for the equation $x^q = a$ in the field of p -adic numbers, [arXiv:1102.2156](#).
- [8] H. Cohen, *Number Theory, Volume I: Tools and Diophantine Equations*, Springer, New York, 2007.
- [9] P.G.O. Freund, E. Witten, Adelic string amplitudes, *Phys. Lett. B* **199** (1987), 191–194.
- [10] F. Q. Gouvea, *p -adic Numbers: An Introduction*, Springer-Verlag, Berlin, 1997.
- [11] K. Hensel, Untersuchung der Fundamentalgleichung einer Gattung für eine reelle Primzahl als Modul und Bestimmung der Theiler ihrer Discriminante, *J. Reine Angew. Math.*, **113** (1894), 61–83.
- [12] A.Yu. Khrennikov, p -adic quantum mechanics with p -adic valued functions, *J. Math. Phys.* **32** (1991) 932–936.
- [13] A. Yu. Khrennikov, *p -Adic Valued Distributions in Mathematical Physics*, Kluwer, Dordrecht 1994.
- [14] A. Kh.Khudoyberdiyev, T.K.Kurbanbaev, B.A.Omirov, Classification of three-dimensional solvable p -adic Leibniz algebras, *P-Adic Numbers Ultrametric Anal. Appl.* **2**(2010) 207–221.
- [15] N. Koblitz, *p -adic numbers, p -adic Analysis, and Zeta Functions*, Springer, New York, 1984.
- [16] S. Lang, *Algebraic Number Theory* Springer-Verlag, New York, 1994.
- [17] Yu. Manin, New dimensions in geometry, *Lect. Notes in Math.*, **1111** (1985), 59–101.
- [18] E. Marinary, G. Parisi, On the p -adic five point function, *Phys. Lett.* **203** (1988) 52–56.
- [19] A. Monna and F. van der Blij, Models of space and time in elementary physics, *J. Math. Anal. and Appl.*, **22** (1968) 537–545.
- [20] F.M. Mukhamedov, U.A. Rozikov, On Gibbs measures of p -adic Potts model on Cayley tree. *Indag. Math. (N.S.)*, **15** (2004) 85–100.
- [21] F.M. Mukhamedov, U.A. Rozikov, On inhomogeneous p -adic Potts model on a Cayley tree. *Inf. Dim. Anal. Quant. Prob. Rel. Fields.* **8**(2005) 277–290.
- [22] F. Mukhamedov, M. Saburov, On equation $x^q = a$ over \mathbb{Q}_p , [arXiv:1106.5935](#).

- [23] J. Neukirch, *Algebraic Number Theory*, Berlin, 1999.
- [24] K.H. Rosen, *Elementary number theory and its applications*, Pearson 2011.
- [25] W.H. Schikhof *Ultrametric calculus: An introduction to p -adic analysis*, Cambridge University Press, 1984.
- [26] J.-P. Serre, *Local Fields*, Sipspringer-Verlag, New York , 1979.
- [27] J.-P. Serre, On a Theorem of Jordan, *Bulletin of AMS* **40** (2003) 429–440.
- [28] Z.H. Sun, On the theory of cubic residues and nonresidues, *Acta Arith.*, **84** (1998), 291–335.
- [29] Z.H. Sun, Cubic and quartic congruences modulo a prime, *J. Num. Theory*, **102** (2003) 41–89.
- [30] Z.H. Sun, Cubic residues and binary quadratic forms, *J. Num. Theory*, **124** (2007) 62–104.
- [31] V. S. Vladimirov, I. V. Volovich, I. Zelenov, *p -Adic Analysis and Mathematical Physics*, World Scientific, Singapore 1994.
- [32] I.V. Volovich, p -adic strings, *Class. Quantum Gray.*, **4** (1987), 83–87.

FARRUKH MUKHAMEDOV, DEPARTMENT OF COMPUTATIONAL & THEORETICAL SCIENCES,
FACULTY OF SCIENCES, INTERNATIONAL ISLAMIC UNIVERSITY MALAYSIA, P.O. Box, 141, 25710,
KUANTAN, PAHANG, MALAYSIA

E-mail address: far75m@yandex.ru

BAKHROM OMIROV, INSTITUTE OF MATHEMATICS AND INFORMATION TECHNOLOGIES,
TASHKENT, UZBEKISTAN

E-mail address: omirovb@mail.ru

MANSOOR SABUROV, DEPARTMENT OF COMPUTATIONAL & THEORETICAL SCIENCES, FAC-
ULTY OF SCIENCE, INTERNATIONAL ISLAMIC UNIVERSITY MALAYSIA, P.O. Box, 141, 25710,
KUANTAN, PAHANG, MALAYSIA

E-mail address: msaburov@gmail.com